



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 143 722 A1

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:

10.10.2001 Bulletin 2001/41

(51) Int Cl.7: H04N 5/913

(21) Application number: 00201277.1

(22) Date of filing: 07.04.2000

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(71) Applicant: Irdeto Access B.V.  
2132 HD Hoofddorp (NL)

(72) Inventor: Wajs, Andrew Augustine  
2023 AA Haarlem (NL)

(74) Representative:  
de Vries, Johannes Hendrik Fokke  
De Vries & Metman  
Overschiestraat 180  
1062 XK Amsterdam (NL)

### (54) Data scrambling and descrambling system

(57) A system for providing scrambled content, comprising a control word generator, each control word including a control word identifier, a scrambler for providing a stream of scrambled data packets, and an encryption device for providing entitlement control messages (ECM's). One or more consecutive packets are scrambled using the same control word (CW). Each packet includes a control word identifier identifying the control word used. The ECM encryption device provides ECM's including a previous control word ( $CW_P$ ), a current control word ( $CW_C$ ) and a next control word ( $CW_N$ ). A system for descrambling scrambled content comprises a descrambler for descrambling the scrambled content and a decryption device for decrypting ECM's to obtain control words. The ECM decryption device delivers

control words to the descrambler and the descrambler descrambles the data packets of the scrambled content using a control word having a control word identifier corresponding with the control word identifier of the data packet to be descrambled. The system further comprises a storage device for storing scrambled content and means to control play back of the stored content, going fast forward and going backwards. The system is programmed to extract ECM's and to provide the ECM's to the ECM decryption device for decryption. The system is programmed to request the ECM decryption device to provide at least a next control word ( $CW_N$ ) at play back or going fast forward, and to provide at least a previous control word ( $CW_P$ ) and a current control word ( $CW_C$ ) at going backwards.

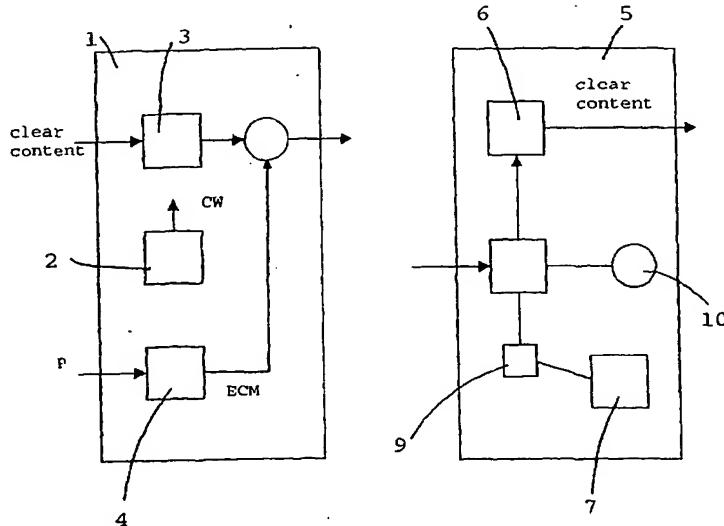


Fig. 1

**Description**

**[0001]** The invention relates to conditional access systems suitable for receiving apparatus provided with storage devices with large capacity. The invention specifically relates to a system for providing scrambled content according to the preamble of claim 1 and to a system for descrambling scrambled content according to the preamble of claim 3.

**[0002]** Recently television receiving apparatus have been equipped with storage devices with large capacity allowing the users to store hours of video content. In this manner the user can create a "personal television" recording his favourite programs and the like. Such receiving apparatus can be made as a television apparatus, a set-top box or the like.

**[0003]** The content stored in the storage devices, such as large hard discs, can include scrambled content with conditional access, wherein control words are needed to descramble the content. Such storage devices allow going backwards through the scrambled content, wherein however the presently available mechanisms for cycling control words become difficult to use. Going backwards is necessary as the users would like to use a VCR-like rewind functionality. However the current techniques used for control word cycling are designed for signals that go forward only.

**[0004]** The invention aims to provide a system for providing scrambled content and a system for descrambling scrambled content of the above-mentioned type, wherein a VCR-like rewind function is supported.

**[0005]** According to the invention a system for providing scrambled content, comprises a control word generator, each control word including a control word identifier, a scrambler for providing a stream of scrambled data packets, wherein one or more consecutive packets are scrambled using the same control word (CW) and wherein each packet includes a control word identifier identifying the control word used, and an encryption device for providing entitlement control messages (ECM's), each ECM including at least a next control word ( $CW_N$ ), characterized in that the ECM encryption device provides ECM's including a previous control word ( $CW_P$ ), a current control word ( $CW_C$ ) and a next control word ( $CW_N$ ).

**[0006]** In a second aspect of the invention a system for descrambling scrambled content is provided, comprising a descrambler for descrambling the scrambled content, a decryption device for decrypting ECM's to obtain control words, wherein the ECM decryption device delivers control words to the descrambler, wherein the descrambler descrambles the data packets of the scrambled content using a control word having a control word identifier corresponding with the control word identifier of the data packet to be descrambled, the system further comprising a storage device for storing scrambled content and a processing unit with means to control playback of the stored content, going fast forward and

going backwards, wherein the processing unit is programmed to extract ECM's and to provide the ECM's to the ECM decryption device for decryption, characterized in that the processing unit is programmed to request the ECM decryption device to provide at least a next control word ( $CW_N$ ) at play back or going fast forward, and to provide at least a previous control word ( $CW_P$ ) and a current control word ( $CW_C$ ) at going backwards.

**[0007]** By providing entitlement control messages with three control words, i.e. the current, next and previous control words, the receiving apparatus can playback stored content from disc in a normal manner, wherein further fast forward and rewind functions are available. When the receiving apparatus is going backwards through the content, the processing unit picks up the first ECM it finds, sends the ECM to the ECM decryption device and requests the decryption device to deliver current and previous keys and loads these keys into the descrambler. Processing the ECM's and synchronizing the provision of control words is relatively simple in this manner.

**[0008]** The invention will be further explained by reference to the drawings in which an embodiment of the systems of the invention is shown.

**[0009]** Fig. 1 shows a simplified diagram of embodiments of the system for providing scrambled content and the system for descrambling scrambled content according to the invention.

**[0010]** Fig. 2 shows a diagram to explain the operation of the systems of the invention.

**[0011]** Fig. 1 shows a system 1 for providing scrambled content comprising a control word generator 2 and a scrambler 3. The scrambler 3 receives clear content and delivers content scrambled using the control words provided by the control word generator 2 as encryption keys. The control word generator provides a new control word every ten seconds for example. As is well-known in the art, the control words are generally used as a seed for a pseudo-random binary sequence generator, wherein the output of the PRBS generator is used for scrambling the clear content. Of course other scramble systems such as a block cypher system may also be used. As such scrambling systems are known per se, this is not discussed in detail in this specification as it is not part of the present invention. Each control word CW has an associated control word identifier, which in case of the generally used MPEG system is only one bit, i.e. either a zero or a one. In a corresponding manner the same control word identifier, i.e. a zero or a one, is associated with each scrambled data packet or plurality of scrambled data packets scrambled under the control of the control word having the same associated identifier zero or one.

**[0012]** The control words  $CW_0$  and  $CW_1$ , are also delivered to an ECM encryption device 4 which encrypts the control words using an input key P. The encryption device 4 can be made as a smart card. The encrypted

ECM's with the control words are inserted into the scrambled content and broadcasted or delivered in any other manner to a number of subscribers each having a system 5 for descrambling scrambled content.

[0013] It is noted that the key P used by the encryption device 4 can be transferred to the systems 5 in so-called entitlement management messages which are not shown in fig. 1. Conditional access systems operating with such a hierarchy of keys are known per se and are not further described in this specification.

[0014] The descrambling system 5 comprises a descrambler 6 for descrambling the scrambled content and a decryption device 7 for decrypting ECM's to obtain the control words CW. This device 7 can be made as a smart card. Further, the system 5 comprises a processing unit 8 controlling the operation of the system and having a schematically indicated control means 9 allowing control of the system by the user. The scrambled content is received by the processing unit 8 and can be stored on a storage device 10, for example a hard disc with large capacity. The processing unit 8 forwards the scrambled content to the descrambler 6 and extracts the ECM's from the stream and forwards the ECM's to the decryption device 7. The decryption device 7, generally made as a secure device such as a smart card, decrypts the ECM's received and as controlled by the processing unit 8 delivers the control words CW<sub>0</sub>, CW<sub>1</sub> to the descrambler 6. If a data packet with the control word identifier 0 is received the control word CW<sub>0</sub> is used, if a data packet having the control word identifier 1 is received, the control word CW<sub>1</sub> is used.

[0015] In the known conditional access system either the current control word CW<sub>C</sub> and the next control word CW<sub>N</sub> is included in the ECM's or only the next control word CW<sub>N</sub>. The decryption device 7 decrypts the control words and loads the control words into the descrambler 6. As stated above, the data packets passing the descrambler 6 have corresponding control word identifiers indicating which control word CW<sub>1</sub> or CW<sub>0</sub> to use. In normal use, when only going forward, an ECM is extracted from the stream and will at least contain the control word CW<sub>1</sub> or CW<sub>0</sub> to be used at the next transition from identifier 1 to 0 in the data packet stream. However when going backwards through the data stream, the ECM at any location will not have the control word CW<sub>P</sub> for the previous data packet. This means that the processing unit 8 must look further back than the current data packet being processed by the descrambler in order to find a previous ECM. This would require an intensive operation and would mean a high load on the processing capacity of the system 5.

[0016] According to the invention, this problem of locating an ECM in the data stream is avoided by including in the ECM's three keys, i.e. the previous control word CW<sub>P</sub>, the current control word CW<sub>C</sub> and the next control word CW<sub>N</sub>. In this manner each ECM extracted from the stream by the processing unit 8 at play back of the content stored on the disc 10 contains three control words,

including the control word required for descrambling the previous data packet. In this manner a rewind function is supported in an easy manner so that the user can scroll back through the content retrieved from the storage device 10 using the control means 9. Of course, such control means may include a remote control device.

[0017] An illustration of the operation of the systems of the invention is schematically shown in fig. 2. A content stream with data packets A, B, C and D is shown, wherein it is assumed that data packet A has the control word identifier 0, the data packet B the identifier 1, the data packet C the identifier 0 etc. The ECM stream is shown above the data packet stream. As indicated, a new ECM is extracted from the stream shortly before a transition from data packet A to B, from B to C etc. The ECM extracted from the data stream shortly before the beginning of data packet A, includes the previous control word CW<sub>P1</sub>, the current control word CW<sub>A0</sub>, and the next control word CW<sub>B1</sub>. The next ECM includes the previous control word CW<sub>A0</sub>, the current control word CW<sub>B1</sub> and the next control word CW<sub>C0</sub>. During normal playback, the processing unit 8 will extract the ECM's subsequently from the data stream and will send the ECM's to the decryption device 7. The processing unit 8 will request the decryption device 7 to send the current control word CW<sub>A0</sub> and the next control word CW<sub>B1</sub> to the descrambler 6. The descrambler 6 receiving the data packet A with identifier 0, will use the control word CW<sub>A0</sub> to descramble this data packet. At the transition from data packet A to data packet B, the new identifier 1 indicates the descrambler 6 to use the control word CW<sub>B1</sub>. The same operation applies to the fast forward mode wherein the processing unit 8 will request the decryption device 7 to send the current and next control words to the descrambler 6.

[0018] If the user operates the control means 9 for going backwards, i.e. a VCR-like rewind function, the processing unit 8 instructs the decryption device 7 to provide the current control word CW<sub>A0</sub> and previous control word CW<sub>P1</sub>. In this manner the descrambler 6 can descramble the previous data packet.

[0019] In the above example it is indicated that the ECM's are stored as part of the content. It is also possible to store the ECM's separately with timing information. In this case timing information in the content stream is used by the processing unit 8 to extract or retrieve the correct ECM's from the storage device 10.

[0020] From the above it will be understood that the invention provides systems, wherein going backwards through the stored video content is allowed without any significant increase in the load on the processing unit in processing ECM's and synchronizing control words. It will be clear that the invention can be used with any type of video or audio content.

[0021] The invention is not restricted to the above described embodiments which can be varied in a number of ways within the scope of the attached claims.

**Claims**

1. System for providing scrambled content, comprising a control word generator, each control word including a control word identifier, a scrambler for providing a stream of scrambled data packets, wherein one or more consecutive packets are scrambled using the same control word (CW) and wherein each packet includes a control word identifier identifying the control word used, and an encryption device for providing entitlement control messages (ECM's), each ECM including at least a next control word (CW<sub>N</sub>), **characterized in that** the ECM encryption device provides ECM's including a previous control word (CW<sub>P</sub>), a current control word (CW<sub>C</sub>) and a next control word (CW<sub>N</sub>).  
5
2. System according to claim 1, wherein the ECM encryption device is accommodated in a smart card.  
20
3. System for descrambling scrambled content, comprising a descrambler for descrambling the scrambled content a decryption device for decrypting ECM's to obtain control words, wherein the ECM decryption device delivers control words to the descrambler wherein the descrambler descrambles the data packets of the scrambled content using a control word having a control word identifier corresponding with the control word identifier of the data packet to be descrambled, the system further comprising a storage device for storing scrambled content and a processing unit with means to control play back of the stored content, going fast forward and going backwards, wherein the processing unit is programmed to extract ECM's and to provide the ECM's to the ECM decryption device for decryption, **characterized in that** the processing unit is programmed to request the ECM decryption device to provide at least a next control word (CW<sub>N</sub>) at play back or going fast forward, and to provide at least a previous control word (CW<sub>P</sub>) and a current control word (CW<sub>C</sub>) at going backwards.  
25  
30  
35  
40
4. System according to claim 3, wherein the processing unit is programmed to request the ECM decryption device to provide the current control word (CW<sub>C</sub>) together with a next control word (CW<sub>N</sub>) at playback or going fast forward and to provide the current control word (CW<sub>C</sub>) together with a previous control word (CW<sub>P</sub>) at going backwards.  
45  
50
5. System according to claim 3 or 4, wherein the ECM decryption device is accommodated in a smart card.  
55

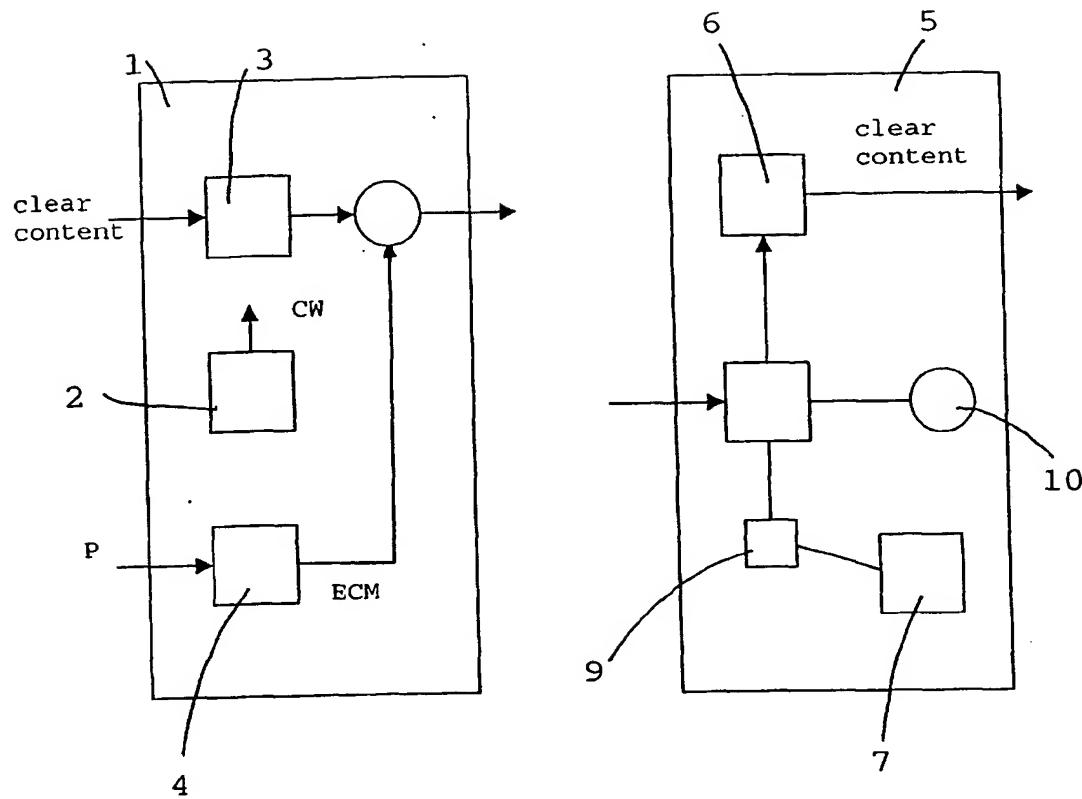


Fig. 1

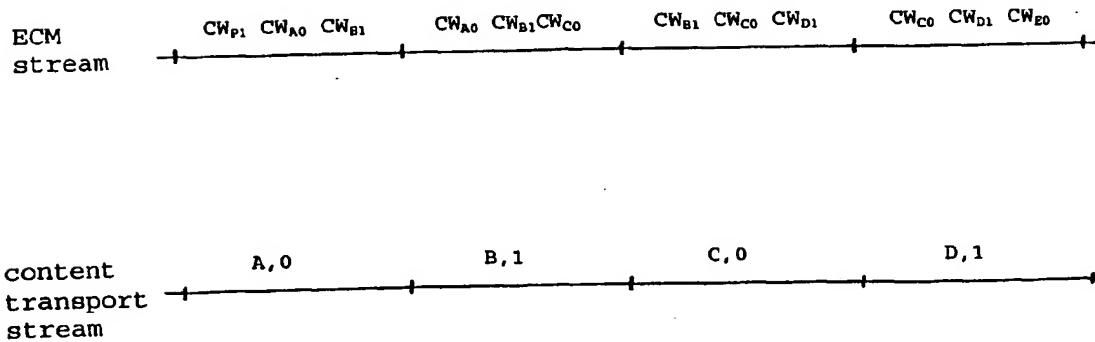


Fig. 2



European Patent  
Office

## **EUROPEAN SEARCH REPORT**

Application Number

DOCUMENTS CONSIDERED TO BE RELEVANT					
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)		
A	EP 0 773 681 A (LG ELECTRONICS INC) 14 May 1997 (1997-05-14) * column 3, line 24 - column 6, line 51; figures 2-6 * ---	1-5	H04N5/913		
A	EP 0 577 365 A (SONY CORPORATION) 5 January 1994 (1994-01-05) * page 10, line 56 - page 11, line 49; figure 2 * -----	1-5			
			<p>TECHNICAL FIELDS SEARCHED (Int.Cl.7)</p> <p>H04N</p>		
<p>The present search report has been drawn up for all claims</p>					
Place of search	Date of compilation of the search	Examiner			
BERLIN	29 August 2000	Dudley, C			
CATEGORY OF CITED DOCUMENTS					
X : particularly relevant if taken alone	T : theory or principle underlying the invention				
Y : particularly relevant if combined with another document of the same category	E : earlier patent document, but published on, or after the filing date				
A : technological background	D : document cited in the application				
O : non-written disclosure	L : document cited for other reasons				
P : intermediate document	& member of the same patent family, corresponding document				

**ANNEX TO THE EUROPEAN SEARCH REPORT  
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 20 1277

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.  
 The members are as contained in the European Patent Office EDP file on  
 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-08-2000

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 0773681 A	14-05-1997	KR	186210 B	15-04-1999
		JP	2933533 B	16-08-1999
		JP	9154101 A	10-06-1997
		US	5832084 A	03-11-1998
<hr/>				
EP 0577365 A	05-01-1994	JP	6078289 A	18-03-1994
		AT	191598 T	15-04-2000
		AU	4159893 A	06-01-1994
		CA	2099175 A	30-12-1993
		CN	1090696 A,B	10-08-1994
		DE	69328277 D	11-05-2000
		ES	2145031 T	01-07-2000
		US	5666461 A	09-09-1997
<hr/>				

**THIS PAGE BLANK (USPTO)**